

PUB-NO: FR002728372A1

DOCUMENT-IDENTIFIER: FR 2728372 A1

TITLE: Securing of payments involving written document

----- KWIC -----

Abstract Text - FPAR (1):

CHG DATE=19990617 STATUS=O>The method of securing payment by written documents such as cheques and drafts uses data written on the document by the payer. The data is an alphanumeric code and a seal code computed from the alphanumeric code and other data entered on document. A seal (8) is calculated from the data (3,4,5) recorded by the payer and printed on the document. The seal is calculated using an algorithm associated with a suitable seal key (7). The algorithm is irreversible. The payment is authorised by reading the alphanumeric code and the seal code from the document and applying the seal algorithm and seal key. The results are compared with the values on the document and if they correspond payment is authorised.

Inventor Name ( Derived ) - INZZ (1):

BOURDIN, MICHEL PAUL

(19) RÉPUBLIQUE FRANÇAISE  
INSTITUT NATIONAL  
DE LA PROPRIÉTÉ INDUSTRIELLE  
PARIS

(11) N° de publication : 2 728 372  
(à n'utiliser que pour les commandes de reproduction)  
(21) N° d'enregistrement national : 94 15060  
(51) Int Cl<sup>e</sup> : G 07 D 7/00, G 06 K 5/00, 9/00

**CETTE PAGE ANNULE ET REMPLACE LA PRECEDENTE**

(12)

**DEMANDE DE BREVET D'INVENTION**

**A1**

(22) Date de dépôt : 14.12.94.

(30) Priorité :

(43) Date de la mise à disposition du public de la demande : 21.06.96 Bulletin 96/25.

(56) Liste des documents cités dans le rapport de recherche préliminaire : Se reporter à la fin du présent fascicule.

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : SLIGOS SOCIETE ANONYME — FR.

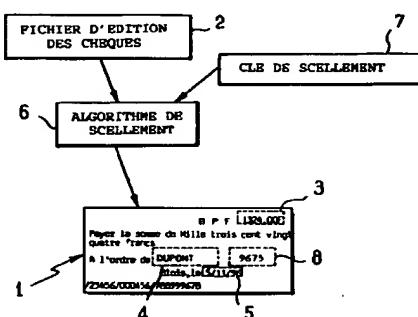
(72) Inventeur(s) : BOURDIN MICHEL PAUL.

(73) Titulaire(s) :

(74) Mandataire : PATCO SA.

**(54) PROCEDE DE SECURISATION DE PAIEMENTS SCRIPTURAUX, DOCUMENT DE PAIEMENT SCRIPTURAL ET PROCEDE DE TRAITEMENT DE PAIEMENTS SCRIPTURAUX SECURISES.**

(57) Le procédé est destiné à sécuriser des paiements scripturaux comportant des données sensibles inscrites sur un document par un émetteur et comporte à cet effet les étapes de calculer un sceau (8) à partir d'au moins une donnée sensible (3, 4, 5) en utilisant un algorithme de scellement associé à une clé de scellement (7) propre à l'émetteur, et d'inscrire le sceau sur le document.



**FR 2 728 372 - A1**



La présente invention concerne un procédé de sécurisation de paiements scripturaux, un document de paiement scriptural sécurisé et un procédé de traitement de paiements scripturaux sécurisés.

5       On entend par paiement scriptural tout paiement effectué par l'inscription sur un document de données sensibles, par exemple l'établissement d'un chèque ou d'un ordre de virement bancaire par l'inscription d'un montant, d'un destinataire désigné par son nom et/ou par ses  
10      références bancaires, et d'une date.

On sait que les grands émetteurs de lettres-chèques telles que les compagnies d'assurances, les mutuelles,... rédigent chaque jour plusieurs milliers de chèques qui sont acheminés par la poste. Ces documents  
15      peuvent être interceptés et modifiés par un fraudeur, en particulier en ce qui concerne le nom du destinataire, ce qui permet au fraudeur d'encaisser le paiement à son profit, éventuellement en modifiant simultanément le montant de ce paiement.

20       A ce propos, on connaît des cas tristement célèbres de chèques dont le nom du destinataire a été modifié par adjonction de syllabes ou de mots supplémentaires permettant l'encaissement du chèque sur un compte dont le titulaire avait en apparence un nom sensiblement  
25      différent de celui du destinataire réel.

L'émission de faux chèques est particulièrement recherchée pour les chèques de banque en raison de la confiance que leur accordent les destinataires qui n'hésitent pas à se séparer de la marchandise réglée par un tel  
30      chèque. A ce propos il convient de noter que les techniques de fabrication sophistiquées incluant l'utilisation de papiers spéciaux et d'encre sensibles au traitement chimique sont très onéreuses sans constituer pour autant une prévention réelle à la contrefaçon.

35       En outre, ces émetteurs dont les références

bancaires sont largement diffusées couvrent un risque supplémentaire de contrefaçon de leurs documents de paiement par l'établissement de faux chèques ou de faux ordres de virements comportant leurs références bancaires.

5           Par ailleurs, en raison des volumes émis par les grands émetteurs et du délai qui s'écoule nécessairement entre l'émission d'un chèque et son encaissement par le destinataire, il est pratiquement impossible de contrôler de façon immédiate les débits qui sont inscrits sur le  
10 compte de l'émetteur de sorte que les détournements sont généralement perçus soit lors d'une réclamation du destinataire qui n'a pas reçu son chèque, soit lors d'un état de rapprochement bancaire révélant qu'un montant erroné a été débité sur le compte de l'émetteur. Dans un cas comme dans  
15 l'autre il est généralement trop tard pour émettre un rejet permettant d'annuler totalement l'opération effectuée.

Selon l'invention on propose un procédé de sécurisation de paiements scripturaux comportant des données sensibles inscrites sur un document par un émet-  
20 teur, ce procédé comportant les étapes de calculer un sceau à partir d'au moins une donnée sensible en utilisant un algorithme de scellement associé à une clé de scellement propre à l'émetteur, et d'inscrire le sceau sur le docu-  
ment.

25           Ainsi, lors du traitement du document, l'organisme tenant le compte de l'émetteur a la possibilité de vérifier l'exactitude du sceau, celui-ci s'avérant incorrect dès l'instant où l'une quelconque des données sensibles ayant servi à l'élaboration du sceau a été modifiée.

30           Selon une version avantageuse de l'invention, l'algorithme de chiffrement est un algorithme irréversible. Ainsi, il n'est pas possible pour un fraudeur connaissant l'algorithme de scellement utilisé de déterminer la clé de scellement par des essais successifs à partir de données  
35 sensibles et du sceau correspondant dont il a eu connais-

sance par suite d'une transaction avec l'émetteur.

Selon un autre aspect de l'invention, on propose un procédé de traitement de paiements scripturaux sécurisés comportant l'étape d'assurer un contrôle du sceau préalablement à l'écriture d'un débit à un compte de l'émetteur. On évite ainsi de pénaliser l'émetteur, même de façon temporaire, pour des opérations effectuées frauduleusement sur son compte.

10 Selon une version avantageuse de cet aspect de l'invention, le contrôle du sceau est déclenché par la reconnaissance d'un numéro de compte d'un émetteur réputé procéder à une sécurisation de paiements scripturaux. On évite ainsi que des fraudeurs puissent encaisser des paiements en omettant le sceau.

15 D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description qui suit en relation avec les figures ci-jointes parmi lesquelles:

- la figure 1 est un schéma synoptique d'élaboration de chèques sécurisés,

- la figure 2 est un schéma synoptique d'un procédé de traitement d'une série de chèques incluant des chèques sécurisés.

En référence à la figure 1, l'élaboration de 25 paiements scripturaux sécurisés selon l'invention, tel qu'un chèque généralement désigné en 1 est effectuée à partir d'un fichier 2 d'édition des chèques contenant des données sensibles telles que le montant 3 des chèques, la désignation du destinataire 4, la date 5, ...

30 Préalablement à l'édition d'un chèque, les données sensibles sont traitées par un algorithme de scellement 6 associé à une clé de scellement 7 propre à l'émetteur.

L'algorithme de scellement 6 est de préférence un 35 algorithme de chiffrement irréversible, par exemple un

algorithme du type DES (abréviation des termes anglais DATA ENSCRIPTION STANDARD). La clé de scellement peut être soit fournie par l'organisme qui tient le compte de l'émetteur, soit élaborée par l'émetteur lui-même et transmise à l'organisme tenant son compte dans des conditions sécurisées. Afin d'augmenter la sécurité, la clé de scellement est de préférence modifiée à des intervalles réguliers, par exemple en effectuant une diversification à partir d'une clé mère conservée dans des conditions de sécurité particulièremenr élevées, seuls les paramètres de diversification étant échangés entre l'émetteur et l'organisme tenant son compte.

Le document édité comporte alors d'une part les données sensibles qui sont transcrives de façon habituelle ainsi qu'un sceau 8 élaboré par l'algorithme de scellement à partir des données sensibles considérées et de la clé de scellement.

La figure 2 illustre le procédé de traitement de paiements scripturaux sécurisés.

Lorsqu'un paquet de documents, ici des chèques 1, revient de la chambre de compensation et doit être traité par un organisme assurant la tenue du compte de différents émetteurs, il est tout d'abord nécessaire d'extraire les chèques des émetteurs ayant opté pour la sécurisation de leurs paiements de façon à s'assurer d'une part que les documents correspondants comportent tous un sceau, ce qui permet de détecter immédiatement les chèques qui sont des contrefaçons ou qui ont été émis à partir de formules vierges volées, et d'autre part que ce sceau est correct.

A cet effet on effectue tout d'abord une reconnaissance 9 du numéro de compte de l'émetteur, par exemple une lecture optique de celui-ci. Si le chèque reçu correspond à un compte non sécurisé, on effectue un débit immédiat 10 du compte et le chèque est ensuite traité de façon habituelle avec la nécessité pour l'émetteur de

procéder très rapidement à un pointage des débits effectués sur son compte et de demander un rejet du paiement dans le cas où une anomalie est constatée, le crédit correspondant ne pouvant être inscrit sur le compte qu'après acceptation 5 du rejet. Dans le cas d'un compte sécurisé, l'organisme tenant le compte effectue une vérification de l'existence d'un sceau et recalcule le sceau à partir des données sensibles inscrites sur le document et de la clé de scellement qui a servi à établir le sceau original et dont 10 il a connaissance par ailleurs. Un contrôle de sceau 11 est effectué. Dans le cas où le sceau s'avère correct, l'organisme tenant le compte peut effectuer un débit 12 du compte. En cas d'absence du sceau ou de sceau incorrect, l'organisme tenant le compte procède au contraire au rejet 15 du document sans débiter le compte de l'émetteur de sorte que la trésorerie de celui-ci ne se trouve pas affectée par la tentative d'opérations frauduleuses sur son compte.

On remarquera que pour une automatisation du procédé de traitement de chèques sécurisés selon l'invention, il est préférable d'inscrire les données sensibles 20 ainsi que le sceau d'une façon permettant une lecture automatique, en particulier une lecture optique.

En pratique, les données sensibles comprennent de préférence le montant du paiement et la désignation du destinataire. Les données sensibles comprennent également 25 de façon avantageuse, la date du paiement de sorte qu'indépendamment de la vérification du sceau il est possible d'effectuer également un recouplement supplémentaire en s'assurant que le compte du destinataire a été ouvert antérieurement à la date du paiement, ce qui permet de 30 détecter les documents volés pour lesquels un compte a été ouvert postérieurement afin d'en effectuer l'encaissement. L'indication de la date permet également de déterminer la clé de scellement à utiliser de sorte qu'une modification 35 frauduleuse de la date entraînera un rejet pour non

conformité du sceau correspondant.

On remarquera que le procédé selon l'invention présente de nombreux avantages tant pour l'émetteur que pour la banque, tous les chèques d'un compte sécurisé étant protégés, y compris les formules vierges en cas de vol ou de contrefaçon, ce qui permet par un changement minime des moyens d'élaboration des paiements scripturaux d'alléger les procédures sécuritaires internes notamment sur la conservation des formules de chèques vierges.

On comprendra que le procédé de sécurisation selon l'invention implique la mise en place des moyens d'élaboration et d'édition du sceau de sorte que ce procédé sera de préférence réservé à des émetteurs professionnels, c'est-à-dire des entreprises ou des personnes physiques traitant un grand volume de paiements scripturaux.

Bien entendu l'invention n'est pas limitée au mode de réalisation décrit.

En particulier, bien que le procédé selon l'invention ait été décrit à propos de l'élaboration de chèques, on peut également traiter de la même façon d'autres paiements scripturaux, en particulier des virements nationaux ou internationaux.

Bien que l'invention ait été décrite en relation avec une édition de chèques à partir d'un fichier, on peut également prévoir de la mettre en oeuvre ponctuellement par édition immédiate d'un document au fur et à mesure de la saisie, le sceau étant établi dès l'instant où toutes les données sensibles utilisées pour son élaboration ont été saisies.

REVENDICATIONS

1. Procédé de sécurisation de paiements scripturaux (1) comportant des données sensibles (3, 4, 5) inscrites sur un document par un émetteur, caractérisé en 5 ce qu'il comporte les étapes de calculer un sceau (8) à partir d'au moins une donnée sensible en utilisant un algorithme de scellement associé à une clé de scellement (7) propre à l'émetteur, et d'inscrire le sceau sur le document.

10 2. Procédé de sécurisation selon la revendication 1, caractérisé en ce que l'algorithme de scellement est un algorithme irréversible.

15 3. Document de paiement scriptural (1) comportant des données sensibles (3, 4, 5) inscrites sur le document, caractérisé en ce qu'il comporte un sceau (8) élaboré à partir d'au moins une des données sensibles.

20 4. Procédé de traitement de paiements scripturaux sécurisés (1), caractérisé en ce qu'il comporte l'étape d'assurer un contrôle (11) du sceau préalablement à l'écriture d'un débit à un compte de l'émetteur.

25 5. Procédé de traitement selon la revendication 4, caractérisé en ce que le contrôle du sceau est déclenché par la reconnaissance (1) d'un numéro de compte d'un émetteur réputé procéder à une sécurisation de paiements scripturaux.

1 / 1

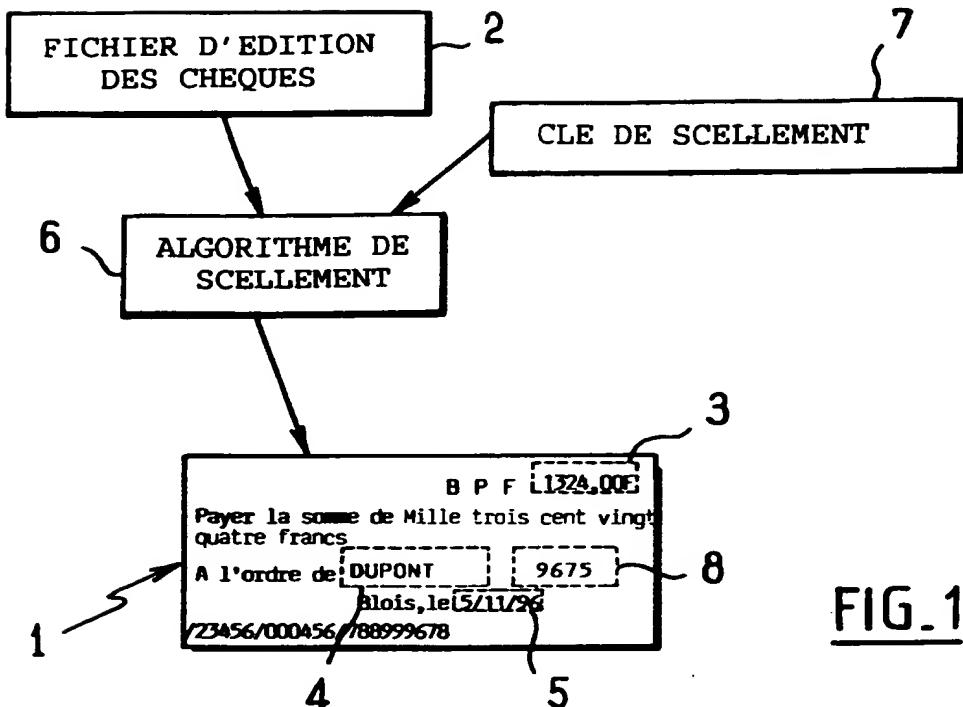


FIG. 1

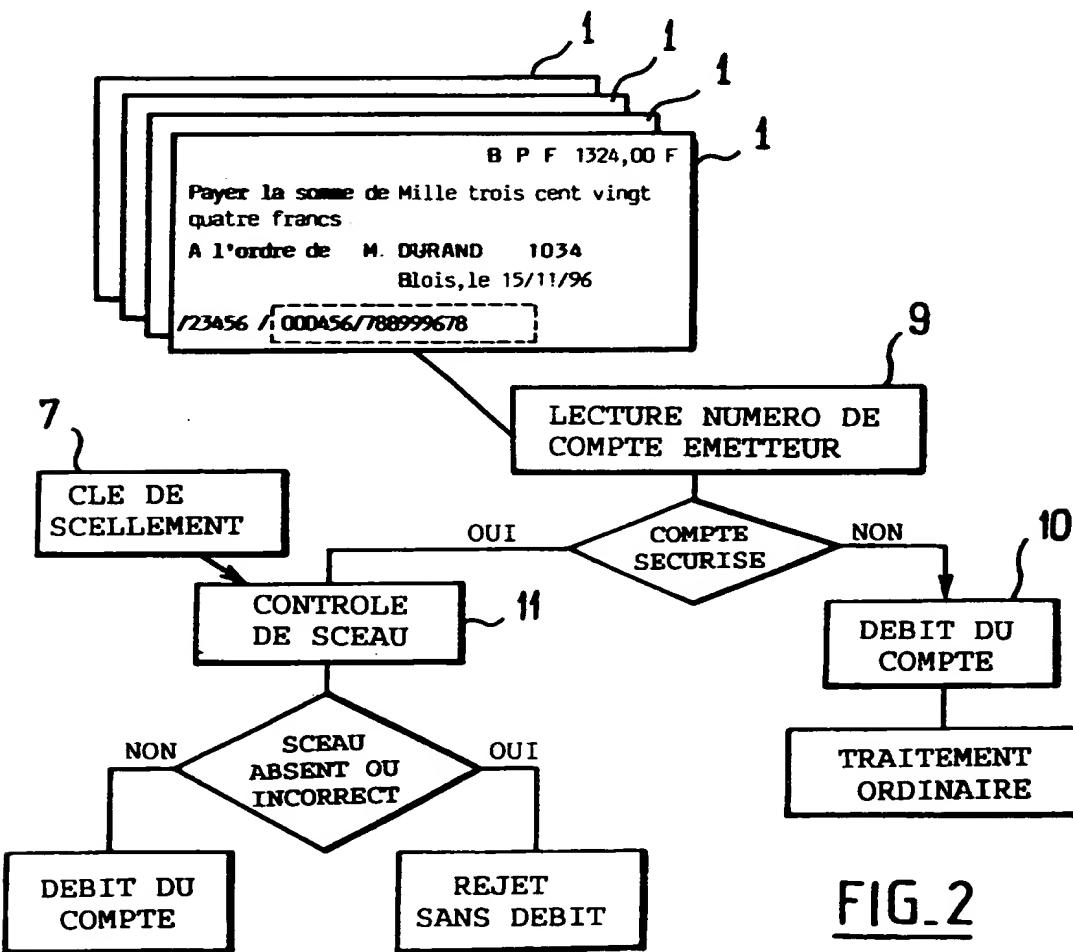


FIG. 2

INSTITUT NATIONAL  
de la  
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE  
PRELIMINAIRE

établi sur la base des dernières revendications  
déposées avant le commencement de la recherche

N° d'enregistrement

FA 508952  
FR 9415060

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications comprises de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
X	FR-A-2 246 913 (GRETAG) * page 3, ligne 21 - page 12, ligne 28; figures *	1,3,4
X	US-A-5 267 314 (L. STAMBLER) * abrégé; figures 6-8,13,14 * * colonne 1, ligne 65 - colonne 2, ligne 49 * * colonne 3, ligne 60 - colonne 8, ligne 2 *	1-4
A	GB-A-2 278 002 (ABATHORN) * abrégé; revendications; figure *	1,3-5
A	EP-A-0 609 937 (BE'ERI PRINTERS)	
		DOMAINES TECHNIQUES RECHERCHÉS (cat.C.I-9)
		G07F G06K
2	Date d'achèvement de la recherche	Exécuteur
	21 Août 1995	David, J
CATEGORIE DES DOCUMENTS CITES		
X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : pertinent à l'encontre d'un autre une revendication ou section-plus technologique générale O : divulgué non écrit P : document intercalaire		T : théorie ou principe à la base de l'invention E : document de brevet délivrant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons R : membre de la même famille, document correspondant